UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,617	07/06/2001	Danny M. Nessett	3COM-3000.WHD.US.CIP	7382

7590 12/21/2004

WAGNER, MURABITO & HAO LLP
Two North Market Street, Third Floor
San Jose, CA 95113

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/900,617	NESSETT ET AL.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-72 are pending in the application.

2. Claims 1-72 have been rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-33 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01.

The omitted steps are: performing a primary authentication protocol.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 12 and 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Vogler et al U.S. Patent No. 6,393,127 B2.

As to claims 1, 12 and 23, Vogler et al discloses a method of protecting communication security when using a key lease to re-authenticate after a primary authentication protocol has been performed, comprising the steps of:

a) performing a secondary authentication protocol between a client electronic system (client) and a network access point electronic system (AP) using the key lease [column 3, lines 41-46]; and

b) if the secondary authentication protocol is successful, generating a session encryption key for encrypting communication traffic between the client and the AP [column 2, lines 42-48].

5. Claims 34-36, 47-49 and 60-62 are rejected under 35 U.S.C. 102(b) as being anticipated by Dabbish et al U.S. Patent No. 5,917,911.

As to claims 34, 47 and 60, Dabbish et al discloses a method of authenticating a client electronic system (client) to allow access to a network, comprising the steps of:

a) in response to a first request to authenticate, performing a primary authentication protocol between the client and a first network access point electronic system (first AP) [column 2, lines 28-49];

b) if the primary authentication protocol is successful, generating a key lease, wherein the key lease includes context information [column 2, lines 50-59];

c) transmitting the key lease to the client [column 4, lines 13-49]; and

d) in response to a second request to authenticate, performing a secondary authentication protocol between the client and a second network access point electronic system (second AP) using the key leas [column 4, lines 13-49]e.

As to claims 35, 48 and 61, Dabbish et al discloses the method further comprising the step of:

e) if the secondary authentication is successful, using the context information of the lease key to control access of the client to the network [column 3 line 50 to column 4 line 12].

As to claims 36, 49 and 62, Dabbish et al discloses that the context information includes information established in the primary authentication protocol [column 2, lines 50-59].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-6, 13-17 and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogler et al U.S. Patent No. 6,393,127 B2 as applied to claims 1, 12 and 23 above, and further in view of Dole U.S. Patent No. 6,628,786 B1.

As to claims 2-5, 13-16 and 24-27, Vogler et al discloses transmitting the key lease from the client to the AP [column 2, lines 42-48]. Vogler et al discloses that the key lease includes an encryption key for use in the secondary authentication protocol [column 2, lines 13-21].

Vogler et al does not teach generating a first random number associated with the client and a second random number associated with the AP. Vogler et al does not teach transmitting the first random number to the AP and the second random number to the client. Vogler et al does not teach using the encryption key, the first random number, the second random number, and a hash function to determine the session encryption key. Vogler et al does not teach applying a HMAC-MD5 algorithm and the encryption key on a concatenation of the first random

number and the second random number to determine the session encryption key. Vogler et al does not teach applying a HMAC-SHA-1 algorithm and the encryption key on a concatenation of the first random number and the second random number to determine the session encryption key.

Dole teaches generating a first random number associated with the client and a second random number associated with the AP [column 6, lines 5-27]. Dole teaches transmitting the first random number to the AP and the second random number to the client [column 6, lines 5-27]. Dole teaches using the encryption key, the first random number, the second random number, and a hash function to determine the session encryption key [column 6, lines 28-36]. Dole teaches applying a HMAC-MD5 algorithm and the encryption key on a concatenation of the first random number and the second random number to determine the session encryption key [column 6 line 50 to column 7 line 2]. Dole teaches applying a HMAC-SHA-1 algorithm and the encryption key on a concatenation of the first random number and the second random number to determine the session encryption key [column 6 line 50 to column 7 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vogler et al so that random numbers would have been generated at the client and the AP. The client's random number would have been transmitted to the AP and the AP's random number would have been transmitted to the client. The two random numbers would have been concatenated. A hashing function and an encryption key would have been applied to the concatenated random numbers. The concatenated random numbers would have been hashed with either a HMAC-MD5 or a HMAC-SHA-1 hashing function.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Vogler et al by the teaching of Dole because this method improves the quality of entropy by allowing machines with no physical source of entropy to gather entropy by communicating with other machines and insure that machines that generate many random session keys do not run the risk of depleting their local supplies of entropy [column 4, lines 45-60].

As to claims 6, 17 and 28, Vogler et al teaches generating a first session encryption key for encrypting communication traffic from the client to the AP. Vogler et al teaches generating a second session encryption key for encrypting communication traffic from the AP to the client.

7. Claims 7-11, 18-22 and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vogler et al U.S. Patent No. 6,393,127 B2 and Dole U.S. Patent No. 6,628,786 B1 as applied to claims 2, 13 and 24 above, and further in view of Kessler et al U.S. Patent No. 6,789,147 B1.

As to claims 7-11, 18-22 and 29-33, the Vogler-Dole combination does not teach using the encryption key, the first random number, the second random number, a first media access control (MAC) address associated with the client, a second media access control (MAC) address associated with the AP, and a hash function to determine the first and second session encryption keys. The Vogler-Dole combination does not teach applying a HMAC-MD5 algorithm and the encryption key on a concatenation of the first random number, the second random number, the first media access control (MAC) address associated with the client, and the second media access control (MAC) address associated with the AP to determine the first session encryption key. The Vogler-Dole combination does not teach applying a HMAC-SHA-1 algorithm and the encryption

key on a concatenation of the first random number, the second random number, the first media access control (MAC) address associated with the client, and the second media access control (MAC) address associated with the AP to determine the first session encryption key. The Vogler-Dole combination does not teach applying a HMAC-MD5 algorithm and the encryption key on a concatenation of the first random number, the second random number, the second media access control (MAC) address associated with the AP, and the first media access control (MAC) address associated with the client to determine the second session encryption key. The Vogler-Dole combination does not teach the Vogler-Dole combination does not teach applying a HMAC-SHA-1 algorithm and the encryption key on a concatenation of the first random number, the second random number, the second media access control (MAC) address associated with the AP, and the first media access control (MAC) address associated with the client to determine the second session encryption key.

Kessler et al teaches using a encryption key, a first random number, a second random number, a first media access control (MAC) address associated with the client, a second media access control (MAC) address associated with the AP, and a hash function to determine a first and second session encryption keys [column 5, lines 18-37]. Kessler et al teaches applying a HMAC-MD5 algorithm and a encryption key on a concatenation of a first random number, a second random number, a first media access control (MAC) address associated with a client, and a second media access control (MAC) address associated with a AP to determine a first session encryption key [column 7 line 54 to column 8 line 10]. Kessler et al teaches applying a HMAC-SHA-1 algorithm and a encryption key on a concatenation of a first random number, a second random number, a first media access control (MAC) address associated with a client, and a

second media access control (MAC) address associated with a AP to determine a first session encryption key [column 7 line 54 to column 8 line 10]. Kessler et al teaches applying a HMAC-MD5 algorithm and a encryption key on a concatenation of a first random number, a second random number, a second media access control (MAC) address associated with a AP, and a first media access control (MAC) address associated with a client to determine a second session encryption key [column 7 line 54 to column 8 line 10]. Kessler et al teaches applying a HMAC-SHA-1 algorithm and a encryption key on a concatenation of a first random number, a second random number, a second media access control (MAC) address associated with a AP, and a first media access control (MAC) address associated with a client to determine a second session encryption key [column 7 line 54 to column 8 line 10].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Vogler-Dole combination so that a encryption key, a first random number, a second random number, a first media access control (MAC) address associated with the client, a second media access control (MAC) address associated with the AP, and a hash function would have been used to determine a first and second session encryption keys. The first session encryption key would have been determined by applying either a HMAC-MD5 or HMAC-SHA-1 hashing function and a encryption key to the concatenation of a first random number, a second random number, a first media access control (MAC) address associated with a client, and a second media access control (MAC) address associated with a AP. The second session encryption key would have been determined by applying either a HMAC-MD5 or HMAC-SHA-1 hashing function and a encryption key to the concatenation of a first random number, a second random number, a first media access control

(MAC) address associated with a client, and a second media access control (MAC) address associated with a AP.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Vogler-Dole combination by the teaching of Kessler et al because it provides a system that does not require a large amount of resources to be consumed with establishing secure sessions and it reduces latency and provides enhanced security [column 2, lines 27-39].

8. Claims 37, 50 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish et al U.S. Patent No. 5,917,911 as applied to claims 34, 47 and 60 above, and further in view of Kennelly et al U.S. Patent No. 6,754,702 B1.

As to claims 37, 50 and 63, Dabbish et al does not teach that the context information includes accounting information, session timeout information, and filtering information.

Kennelly et al teaches context information that includes accounting information, session timeout information, and filtering information [column 14, lines 36-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al so that the context information would have included account information, session time out information and system filtering information.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al by the teaching of Kennelly et al because it helps organize which resources of a network device can be allocated between organizations or users [column 2, lines 8-14].

9. Claims 38-43, 51-56 and 64-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish et al U.S. Patent No. 5,917,911 as applied to claims 34, 47 and 60 above, and further in view of Babu et al U.S. Patent No. 6,122,639.

As to claims 38, 41, 43, 51, 54, 56, 64, 67 and 69, Dabbish et al discloses that the key lease further includes a first identifier associated with the client [column 4, lines 50-67]. Dabbish et al discloses a first encryption key associated with the primary authentication protocol [column 5, lines 1-23]. Dabbish et al discloses a second encryption key for use in the secondary authentication protocol [column 5, lines 43-53]. Dabbish et al discloses a key lease period for indicating a length of time in which the key lease is valid [column 8, lines 48-60]. Dabbish et al discloses a second identifier associated with a particular network access point electronic system group of a plurality of network access point electronic system groups [column 7, lines 24-39].

Dabbish et al does not teach an integrity function data for determining an unauthorized change to a first portion of the key lease.

Babu et al teaches an integrity function data for determining an unauthorized change to a first portion of the key lease [column 9 line 61 to column 10 line 5].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al so that there would have been means for determining unauthorized change to the first portion of the key lease.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al by the teaching of Kennelly et al because it ensures that a third party did not intercept the keys and modify them [column 4, lines 43-57].

As to claims 39, 52 and 65, Dabbish et al teaches that the first portion includes the first identifier, the first encryption key, the second encryption key, the key lease period, and the context information [column 8, lines 48-60].

As to claims 40, 53 and 66, Dabbish et al teaches that a second portion of the key lease is encrypted using a third encryption key [column 8, lines 36-41].

As to claims 42, 55 and 68, Dabbish et al teaches that step b) includes:

b1) transmitting the first identifier and the key lease to the second AP [column 4, lines 50-67];

b2) if the second AP is associated with the second identifier of the key lease, retrieving the third encryption key corresponding to the second identifier [column 7, lines 24-39]; and

b3) decrypting the second portion of the key lease using the retrieved third encryption key [column 8, lines 42-47].

10. Claims 44, 57 and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish et al U.S. Patent No. 5,917,911 as applied to claims 34, 47 and 60 above, and further in view of Kung et al U.S. Patent No. 5,434,918.

As to claims 44, 57 and 70, Dabbish et al does not teach that the secondary authentication protocol comprises a mutual challenge-response protocol based on symmetric encryption.

Kung et al teaches a secondary authentication protocol that comprises a mutual challenge-response protocol based on symmetric encryption [column 3, lines 16-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al so that the second authentication protocol would have been a mutual challenge-response protocol based on symmetric encryption.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al by the teaching of Kung et al because the use of mutual authentication that employs symmetric encryption provides for network security and will authenticate individual users on client workstations and permit users to authenticate to the AP [column 2, lines 19-26].

11. Claims 45, 58 and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish et al U.S. Patent No. 5,917,911 as applied to claims 34, 47 and 60 above, and further in view of Burns et al U.S. Patent No. 6,792,424.

As to claims 45, 58 and 71, Dabbish et al does not teach that the secondary authentication protocol comprises a mutual challenge-response protocol based on a one-way hash function message authentication code (HMAC) implementation.

Burns et al teaches a secondary authentication protocol that comprises a mutual challenge-response protocol based on a one-way hash function message authentication code (HMAC) implementation [column 6 line 49 to column 7 line 6].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al so that that the secondary authentication protocol would have been a mutual challenge-response protocol based on a one-way hash function message authentication code (HMAC) implementation.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al by the teaching of Burns et al because it ensures the correctness of the actions while minimizing computational overhead [column 6 line 49 to column 7 line 6].

12. Claims 46, 59 and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish et al U.S. Patent No. 5,917,911 as applied to claims 34, 47 and 60 above, and further in view of Burns et al U.S. Patent No. 6,792,424.

As to claims 46, 59 and 72, Dabbish et al does not teach that the secondary authentication protocol comprises a mutual challenge-response protocol based on a keyed message authentication code implementation.

Burns et al teaches a secondary authentication protocol that comprises a mutual challenge-response protocol based on a keyed message authentication code implementation [column 6 line 49 to column 7 line 6].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al so that that the secondary authentication protocol would have been a mutual challenge-response protocol based on a keyed message authentication code implementation.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dabbish et al by the teaching of Burns et al because it ensures the correctness of the actions while minimizing computational overhead [column 6 line 49 to column 7 line 6].

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
December 15, 2004

AU 2131
12/16/04